Exhibit J

CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER

RIDGEVIEW MEDICAL CENTER AND CLINICS #3517

SUBJECT: PHYSICAL SECURITY POLICY

ORIGINATING DEPT: Information Technology (IT) **DISTRIBUTION DEPTS:** All

ACCREDITATION/REGULATORY STANDARDS:

Original Date: 12/12 **Revision Dates:** **Reviewed Dates:**	**APPROVAL:** Administration: _____ Director: _____

PURPOSE:

The purpose of the Ridgeview Medical Center Physical Security Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

Audience

The Ridgeview Medical Center Physical Security Policy applies to all Ridgeview Medical Center individuals that install and support Information Resources, are charged with Information Resource security and data owners.

POLICY:

- Physical security systems must comply with all applicable regulations including but not limited to building codes and fire prevention codes.
- Physical access to all Ridgeview Medical Center restricted facilities must be documented and managed.
- All Information Resource facilities must be physically protected in proportion to the criticality or importance of their function at Ridgeview Medical Center.
- Access to Information Resources facilities must be granted only to Ridgeview Medical Center support personnel and contractors whose job responsibilities require access to that facility.
- The process for granting card and/or key access to Information Resource facilities must include the approval of the person responsible for physical facility management.
- Each individual that is granted access rights to an Information Resource facility must sign the appropriate access and non-disclosure agreements.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for Information Resource physical facility management. Cards must not be reallocated to another individual, bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for Information Resource physical facility management as soon as practicable.
- Cards and/or keys must not have identifying information other than a return mail address.
- All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.

Confidential

- Card access records and visitor logs for Information Resource facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- The person responsible for Information Resource physical facility management must remove the card and/or key access rights of individuals that change roles within Ridgeview Medical Center or are separated from their relationship with Ridgeview Medical Center
- Visitors in card access controlled areas of Information Resource facilities must be accompanied by authorized personnel at all times.
- The person responsible for Information Resource physical facility management must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for Information Resource physical facility management must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

WAIVERS:
Waivers from certain policy provisions may be sought following the process outlined in the Ridgeview Medical Center Policy #3511 – *Enterprise Information Security Governance*.

ENFORCEMENT:
Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights and termination of contract(s).

VERSION HISTORY OF SOURCE DOCUMENT: Ridgeview Medical Center Information Security Policy Manual

Version Number	Date	Reason/Comments
V1.00	December, 2012	Document Origination
V2.00	May, 2014	Full review with IT Steering Committee
V3.00	August, 2015	Reviewed with Security Committee
	6/16	Finalized, assigned policy number, on RidgeNet. Previous documentation not archived.

Confidential